Naciones Unidas A/CN.9/630/Add.3

Asamblea General

Distr. general
16 de abril de 2007
Español
Original: inglés

Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
40º período de sesiones
Viena, 25 de junio a 12 de julio de 2007

Posible labor futura en la esfera del comercio electrónico

Documento general de referencia sobre los elementos necesarios para establecer un marco jurídico favorable al comercio electrónico: modelo de capítulo sobre la utilización internacional de métodos de autenticación y firma electrónicas

Nota de la Secretaría

Adición

En el anexo de la presente nota figura una parte (segunda parte, seccs. A y B del Cap. I) de un modelo de capítulo de un documento general de referencia sobre el tema de las cuestiones jurídicas relacionadas con la utilización internacional de los métodos de autenticación y firma electrónicas.

V.07-82262 (S) 110507 150507

Anexo

Índice

Segunda Parte

Utilización transfronteriza de los métodos de firma y autenticación electrónicas

I. Reconocimiento jurídico de los métodos de autenticación y firma electrónicas extranjeros

1. Las incompatibilidades jurídicas y técnicas son las dos causas principales de dificultades en la utilización transfronteriza de los métodos de firma y autenticación electrónicas, en particular cuando su finalidad es sustituir una firma legalmente válida. Las incompatibilidades técnicas son las que afectan a la interoperatividad de los sistemas de autenticación. Las incompatibilidades jurídicas pueden surgir cuando las leyes de los diferentes ordenamientos estipulan diferentes requisitos en cuanto a la utilización y la validez de los métodos de firma y autenticación electrónicas.

A. Repercusión internacional de la legislación interna

2. Cuando la legislación interna admite formas electrónicas equivalentes a los métodos de autenticación basados en un soporte de papel, es posible que sean incompatibles los criterios de validez de esas formas electrónicas equivalentes. Por ejemplo, si la ley reconoce sólo las firmas digitales, no serán aceptables otras formas de firma electrónica. Puede ser que otras discrepancias en los criterios de reconocimiento de los métodos de autenticación y firma electrónicas no impidan en principio su utilización a través de las fronteras, pero el costo y las molestias resultantes de la necesidad de satisfacer los requisitos prescritos por los diversos ordenamientos tal vez reduzcan las ventajas de rapidez y eficiencia que es de esperar reporte la utilización de las comunicaciones electrónicas.

3. En las siguientes secciones se examinan las repercusiones que tienen diferentes enfoques jurídicos de la tecnología en la expansión del reconocimiento transfronterizo. También se resume el consenso internacional naciente sobre las medidas que tal vez podrían facilitar la utilización internacional de los métodos de firma y autenticación electrónicas.

1. Obstáculos internacionales creados por enfoques nacionales contrapuestos

4. Los enfoques neutrales desde el punto de vista tecnológico, en especial los que incluyen una “prueba de fiabilidad”, tienden a resolver las incompatibilidades legales. Entre los instrumentos jurídicos internacionales que adoptan este enfoque figuran la Ley Modelo de la CNUDMI sobre Comercio Electrónico[1], en el apartado b) del párrafo 1 de su artículo 7, y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales[2], en el párrafo 3 de su artículo 9. Según este enfoque, un método de firma o autenticación electrónicas capaz de identificar al firmante e indicar su intención con

[1] Véase la nota [...] [publicación de las Naciones Unidas, Nº de venta S.99.V.4].
[2] Véase la nota [...] [resolución 60/21 de la Asamblea General, anexo].

respecto a la información concernida en la comunicación electrónica cumple los requisitos de la firma, siempre que satisfaga varios criterios. Atendidas todas las circunstancias del caso, incluso la existencia de un acuerdo entre el iniciador y el destinatario del mensaje de datos, hay que demostrar que el método de firma o autenticación es tan fiable como corresponde a la finalidad para la que se genera o comunica dicho mensaje. Otra posibilidad es la obligación de demostrar que ha cumplido esa finalidad por sí mismo o juntamente con otros medios probatorios.

5. Cabe sostener que el planteamiento minimalista facilita la utilización transfronteriza de la autenticación y la firma electrónicas, pues con arreglo al mismo es posible usar con validez cualquier método de firma o autenticación electrónicas para firmar o autenticar un contrato o comunicación, siempre que satisfaga las anteriores condiciones generales. Sin embargo, la consecuencia de este enfoque es que por lo general esas condiciones se confirman solamente *a posteriori* y no hay ninguna garantía de que un tribunal reconozca la utilización de un método determinado.

6. La utilización transfronteriza de la autenticación y las firmas electrónicas se convierte en un verdadero problema en los sistemas que prescriben imperativamente o dan preferencia a una tecnología determinada. La complejidad del problema aumenta en proporción directa al grado de regulación estatal de las firmas y la autenticación electrónicas y al grado de seguridad jurídica que la ley concede a un método o tecnología determinados. Las razones son simples: cuando la ley no atribuye validez ni presunción jurídica especial alguna a determinados tipos de firma o autenticación electrónicas, y se limita a prescribir su equivalencia general a las firmas manuscritas o a la autenticación sobre soporte de papel, los riesgos de confiar en una firma electrónica son los mismos, conforme a la legislación vigente, que el riesgo de fiarse de una firma manuscrita. En cambio, cuando la ley atribuye más presunciones legales a una firma electrónica determinada (habitualmente a las consideradas “seguras” o “avanzadas”), el grado creciente de riesgo se desplaza de una parte a la otra. Un supuesto fundamental de la legislación con orientación tecnológica específica es que ese desplazamiento general *a priori* del riesgo jurídico puede estar justificado por el grado de fiabilidad que ofrece una tecnología determinada, siempre que se cumplan ciertas normas y ciertos procedimientos. El reverso de este planteamiento es que una vez que se afirma la fiabilidad *a priori* del uso (entre otras condiciones) de una tecnología determinada, todas las demás, o incluso la misma tecnología utilizada en condiciones ligeramente diferentes, se convierten *a priori* en poco fiables, o al menos se hacen sospechosas *a priori* de falta de fiabilidad.

7. Por consiguiente, es posible que una legislación nacional con orientación tecnológica específica discrepante dificulte más que promueva la utilización de las firmas electrónicas en el comercio internacional. Ello podría suceder de dos maneras distintas pero estrechamente relacionadas.

8. Primero, si las firmas electrónicas y los proveedores de servicios de certificación que las autentican están sujetos a requisitos jurídicos y técnicos contradictorios en diferentes ordenamientos, ello puede coartar o impedir la utilización de firmas electrónicas en muchas operaciones transfronterizas, si con esa firma es imposible satisfacer simultáneamente los requisitos de los distintos ordenamientos jurídicos.

9. Segundo, la legislación con orientación tecnológica específica, en especial la que da preferencia a las firmas digitales, lo que también sucede con el enfoque en dos fases, tiende a originar una mezcolanza de normas técnicas y requisitos de autorización contradictorios que dificulta mucho la utilización transfronteriza de firmas electrónicas. Un sistema en el que cada país prescribe sus propias normas puede también impedir que las partes concierten acuerdos de reconocimiento mutuo y certificación cruzada[3]. En efecto, un arduo problema pendiente, relativo en particular a las firmas digitales, es el del reconocimiento transfronterizo. El Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada, de la Organización de Cooperación y Desarrollo Económicos (OCDE) (en lo sucesivo Grupo de Trabajo de la OCDE) ha hecho observar que, si bien el enfoque adoptado por la mayoría de los ordenamientos jurídicos parece ser no discriminatorio, las diferencias de los requisitos a nivel nacional continuarán generando problemas de interoperatividad[4]. A los efectos del presente estudio, pueden ser significativos los siguientes puntos débiles señalados por el Grupo de Trabajo de la OCDE:

a) **Interoperatividad**. Se comprobó que eran frecuentes los problemas y limitaciones en cuanto a interoperatividad. En el plano técnico, aunque abundan las normas, se citó como problema la falta de normas "básicas" comunes a algunas tecnologías. En el plano jurídico/normativo, se señalaron como factores que impedían el progreso la dificultad de los responsables en comprender sus respectivos marcos de confianza mutua, incluso en los temas de asignación de responsabilidad e indemnización. Según el Grupo de Trabajo de la OCDE éste es un ámbito que parece requerir un examen y análisis más a fondo con miras a elaborar tal vez instrumentos comunes que sean útiles a los ordenamientos jurídicos al objeto de lograr el grado de interoperatividad deseado para una aplicación o sistema determinados;

b) **Reconocimiento de los servicios de autenticación extranjeros**. Según el Grupo de Trabajo de la OCDE, la labor se ha centrado en el establecimiento de servicios nacionales. En consecuencia, los mecanismos de reconocimiento de los servicios de autenticación extranjeros no se han desarrollado por lo general muy satisfactoriamente. En estas condiciones, el mencionado Grupo de Trabajo señala que éste parece ser un ámbito en que sería de utilidad proseguir la tarea. Dado que los trabajos en este terreno guardarían estrecha relación con la cuestión más general de la interoperatividad, estos temas podrían combinarse;

c) **Aceptación de credenciales**[5]. En algunos casos, se señaló como impedimento para la interoperatividad la aceptación de las credenciales emitidas por

---

[3] Stewart Baker y Mattehw Yeo, en colaboración con la secretaría de la Unión Internacional de Telecomunicaciones, "Background and issues concerning authentication and the ITU", ponencia informativa presentada a una reunión de expertos sobre firmas electrónicas y autoridades de certificación: cuestiones de telecomunicaciones, celebrada en Ginebra los días 9 y 10 de diciembre de 1999, documento Nº 2.

[4] Organización de Cooperación y Desarrollo Económicos, Grupo de Trabajo sobre la seguridad de la información y la protección de la vida privada, *The Use of Authentication across Borders in OECD Countries* (DSTI/ICCP/REG(2005)4/FINAL), http://www.oecd.org/dataoecd/1/10/35809749.pdf, consultado el 2 de febrero de 2007.

[5] Una credencial es un elemento simbólico dado para probar que una persona o un aparato determinado se ha sometido a un proceso de autenticación. Las credenciales vinculadas al usuario son esenciales a

otras entidades. A este respecto, el Grupo de Trabajo de la OCDE sugiere que podría considerarse la posibilidad de establecer una serie de prácticas óptimas o directrices relativas a la emisión de credenciales con fines de autenticación. Es posible que en diversos ordenamientos jurídicos estén ya en curso trabajos sobre este tema que podrían constituir una útil aportación a eventuales iniciativas del Grupo de Trabajo de la OCDE sobre el particular;

d) **Se utiliza una amplia variedad de métodos de autenticación**. El Grupo de Trabajo de la OCDE constató que prácticamente en todos los Estados Miembros de la Organización se hacía uso de una amplia variedad de soluciones al tema de la autenticación. Los métodos van desde el uso de contraseñas, por una parte, hasta elementos simbólicos, firmas digitales y datos biométricos, por otra. Según sea la aplicación, y los correspondientes requisitos, los métodos pueden utilizarse solos o en combinación. Muchos observadores podrían considerar que ello es positivo, pero la información reunida en el estudio del Grupo de Trabajo de la OCDE da a entender que la gama de posibilidades es tan amplia que existe el riesgo de que los proveedores y usuarios de aplicaciones se vean sumidos en la mayor perplejidad al decidir qué método es el apropiado para sus necesidades. Según el mencionado Grupo de Trabajo, esto parecería indicar que sería en cierto modo ventajoso establecer un instrumento de referencia para evaluar los diversos métodos de autenticación y el grado en que sus características responden a las necesidades constatadas por los proveedores o los usuarios de aplicaciones.

10. La confianza en la utilización de métodos de firma y autenticación electrónicas podría incrementarse con la adopción de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y la aplicación de su enfoque de neutralidad tecnológica a las firmas y la autenticación electrónicas. Ahora bien, es poco realista esperar que ello obviaría por completo la necesidad de una solución armonizada para abordar normativas jurídicas y técnicas incompatibles. Es posible que muchos países sigan prescribiendo el uso de métodos específicos de autenticación en ciertos tipos de operación. También puede ser que algunos países estimen necesaria orientación más concreta para aquilatar la fiabilidad de los métodos de firma y autenticación, en particular los extranjeros, y su equivalencia a los métodos utilizados o al menos conocidos en el país.

2. Gestación de un consenso

11. La divergencia de normativas que se ha dado a nivel internacional es probablemente resultado de una combinación de factores, en grados variables. Como se ha señalado anteriormente (véanse los párrs. [...] a [...] *supra*) algunos países tienden a establecer requisitos más estrictos y particularizados en lo que respecta a las firmas y los documentos, mientras que otros centran su interés en la

---

efectos de identificación. Las credenciales al portador pueden ser suficientes para algunas formas de autorización. Como ejemplos cabe citar un permiso de conducir válido, el número de seguridad social u otro número identificador de una persona, o bien las tarjetas con microcircuito. Centro para la Democracia y la Tecnología, “Privacy principles for authentication systems”, http://tprc.org/papers/2003/183/CDTauthenticationTPRC.pdf, consultado el 12 de abril de 2007; véase también el documento de un grupo de trabajo de dicho Centro sobre principios de protección de la vida privada en materia de autenticación, titulado “Interim report on privacy principles for authentication systems”, http://www.cdt.org/privacy/authentication/030513interim.pdf, consultado el 12 de abril de 2007.

intención de la parte firmante y permiten una extensa variedad de formas de probar la validez de las firmas. Estas diferencias generales suelen traslucirse en la legislación concreta relativa a los métodos de autenticación y firma electrónicas (véanse los párrs. [...] a [...] *supra*). Otra causa de incoherencia es resultado del grado variable de ingerencia de las autoridades nacionales en los aspectos técnicos de dichos métodos. Algunos países tienden a desempeñar un papel directo en el establecimiento de normas sobre nuevas tecnologías, posiblemente en la creencia de que ello confiere una ventaja competitiva a la industria nacional[6].

12. La divergencia de las normativas puede también obedecer a diferentes hipótesis sobre la forma en que cristalizarán las tecnologías de autenticación. En uno de esos supuestos, el llamado "paradigma universal de autenticación"[7], se da por sentado que la finalidad principal de las tecnologías de autenticación será verificar las identidades y características entre personas que no tienen ninguna relación anterior entre sí y cuyo uso común de la tecnología no es el objeto del acuerdo contractual. Por tanto, lo que debe hacer la tecnología de autenticación o firma es confirmar la identidad u otras características de una persona a un número de personas potencialmente ilimitado y para un número de fines potencialmente ilimitado. Este modelo hace hincapié en la importancia de las normas técnicas y de los requisitos operativos de los proveedores de servicios de certificación en el caso de terceros en los que se deposita confianza. Otro marco hipotético, el llamado "paradigma de autenticación limitado" parte del supuesto de que el principal uso de las tecnologías de autenticación y firma será verificar las identidades y características entre personas cuyo uso común de la tecnología se realiza con sujeción a acuerdos contractuales[8]. Por consiguiente, lo que debe hacer la tecnología de autenticación es confirmar la identidad u otras características del poseedor del certificado sólo para una serie de fines concretamente especificados y dentro de una colectividad definida de partes potencialmente confiantes que se someten a condiciones comunes para el uso de la tecnología. Este modelo hace hincapié en el reconocimiento jurídico de los acuerdos contractuales.

13. Pese a estas discrepancias, algunas de las cuales aún predominan, las constataciones del Grupo de Trabajo de la OCDE[9] dan a entender que parece existir ahora un creciente consenso internacional sobre los principios básicos que deben regir el comercio electrónico y en particular la firma electrónica. Para el presente estudio son de especial interés las constataciones siguientes:

a) **Enfoque no discriminatorio de las firmas y servicios "extranjeros"**. Los marcos legislativos no niegan efectividad jurídica a las firmas provenientes de servicios con sede en otros países siempre que esas firmas se hayan creado en las mismas condiciones que aquellas a las que se ha dado efecto legal en el ámbito interno. En tal caso, el enfoque parece ser no discriminatorio, siempre que se satisfagan los requisitos nacionales o su equivalente. Ello concuerda con las constataciones de anteriores estudios sobre la autenticación efectuados por el Grupo de Trabajo de la OCDE;

---

[6] Véase la nota [...] [Antecedentes y cuestiones referentes a la autenticación y la UIT].

[7] Ibíd.

[8] Ibíd.

[9] Véase la nota [...] [*The Use of Authentication across Borders in OECD Countries*].

b) **Neutralidad tecnológica**. Aunque prácticamente todos los que respondieron a la encuesta indicaron que su marco legislativo y reglamentario de los servicios de autenticación y firmas electrónicas era tecnológicamente neutral, la mayoría señaló que, cuando se trataba de aplicaciones electrónicas en la administración pública o cuando se requería la máxima seguridad jurídica de la firma electrónica, se estipulaba la utilización de una infraestructura de clave pública (ICP). En esas condiciones, aunque los marcos legislativos pueden ser tecnológicamente neutros, las decisiones de política parecen exigir la especificación de la tecnología;

c) **Predominio de la ICP**. Según el Grupo de Trabajo de la OCDE, la ICP parece ser el método de autenticación preferido cuando se requieren pruebas sólidas de la identidad y una gran seguridad jurídica de la firma electrónica. Se utiliza en determinadas "comunidades de intereses" cuando todos los usuarios parecen tener una relación comercial previa de alguna forma. El uso de tarjetas con microcircuito habilitadas para la ICP y la integración de funciones de certificación digital en los programas informáticos de aplicaciones han hecho que el empleo de este método sea menos complicado para los usuarios. Sin embargo, se reconoce en general que la ICP no es necesaria para todas las aplicaciones y que la selección de los métodos de autenticación debe efectuarse en función de su adecuación a los fines para los que se utilicen.

14. Además, el Grupo de Trabajo de la OCDE constató que los sistemas reguladores de todos los países estudiados tenían establecida alguna forma de marco legislativo o reglamentario que regulara el efecto jurídico de las firmas electrónicas a nivel nacional. El Grupo de Trabajo comprobó que, si bien los detalles de la legislación podían diferir de unos ordenamientos jurídicos a otros, parecía ser discernible un enfoque uniforme en el sentido de que la mayoría de las leyes internas tenía como base marcos internacionales o transnacionales ya existentes (por ejemplo la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas y la Directiva 1999/93/CE del Parlamento Europeo y del Consejo sobre un marco comunitario para las firmas electrónicas[10]).

B. Criterios de reconocimiento de los métodos extranjeros de autenticación y firma electrónicas

15. Como se ha indicado anteriormente, uno de los principales obstáculos a la utilización transfronteriza de las firmas y la autenticación electrónicas viene siendo la falta de interoperatividad, debida a normas contradictorias o discrepantes o bien a su aplicación falta de concordancia. Se han creado varios foros para promover una ICP normalizada e interoperativa como fundamento de la seguridad de las operaciones en las aplicaciones del comercio electrónico. Entre ellos figuran organizaciones intergubernamentales[11] y mixtas del sector público y el sector privado[12] a nivel mundial[13] o regional.

---

[10] *Diario Oficial de las Comunidades Europeas, L 13/12, 19 de enero de 2000*.

[11] En la región de Asia y el Pacífico, el foro de la Asociación de Cooperación Económica en Asia y el Pacífico (APEC) ha elaborado el documento "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (Grupo de Tareas sobre seguridad electrónica, Grupo de Trabajo de la APEC sobre telecomunicaciones e información, diciembre

16. El objetivo de algunos de estos trabajos es establecer normas técnicas sobre la presentación de la información necesaria para cumplir ciertos requisitos legales[14]. Pero, en gran medida, esta importante labor se ocupa sobre todo de los aspectos técnicos y no de las cuestiones jurídicas, por lo que se sitúa fuera del ámbito del presente estudio. En consecuencia, el análisis efectuado en las secciones siguientes

---

de 2004), http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf, consultado el 12 de abril de 2007. La finalidad de esas directrices es facilitar el establecimiento de sistemas potencialmente interoperativos así como el examen de la interoperatividad de sistemas existentes. Las directrices tratan solamente de las clases o tipos de certificados utilizados en el comercio electrónico transnacional. No tiene por objeto otros certificados ni pretenden limitar los sistemas solamente a la emisión de los certificados que en ellas se contemplan.

[12] En la Unión Europea, la Junta de Normalización en materia de Tecnología de la Información y las Comunicaciones (TIC) creó en 1999 la Iniciativa europea de normas para firmas electrónicas (EESSI) dirigida a coordinar las actividades de normalización en apoyo de la aplicación de la Directiva 1999/93/CE de la Unión Europea, referente a las firmas electrónicas. La Junta de Normalización en materia de TIC es una iniciativa del Comité Europeo de Normalización (CEN), creado por organizaciones de normalización nacionales y dos organizaciones sin fines de lucro; el Comité Europeo de Normalización Electrotécnica y el Instituto Europeo de Normas de Telecomunicación (ETSI). La EESSI ha elaborado varias normas para promover la interoperatividad, pero su aplicación es lenta, supuestamente a causa de su complejidad (Paolo Balboni, "Liability of certification service providers towards relying parties and the need for a clear system to enhance the level of trust in electronic communication", *Information and Communications Technology Law*, vol. 13, Nº 3, 2004, págs. 211 a 242, 214.

[13] Por ejemplo, la Organization for the Advancement of Structured Information Standards (OASIS), consorcio internacional sin fines lucrativos fundado en 1993 para fomentar el desarrollo, la convergencia y la adopción de normas para el comercio electrónico. La OASIS ha establecido un comité técnico sobre ICP, formado por usuarios de ICP, vendedores y expertos, encargado de estudiar las cuestiones relativas a la propagación de la tecnología de certificación digital. Dicho comité técnico ha preparado un plan de acción que prevé, entre otras cosas, la elaboración de directrices o perfiles específicos que describan la forma en que las normas deben utilizarse en determinadas aplicaciones para conseguir la interoperatividad en materia de ICP, crear nuevas normas cuando sea necesario, y prever pruebas de interoperatividad y actos de comprobación (OASIS, comité técnico sobre ICP, "plan de acción ICP", febrero de 2004), http://www.oasis-open.org/committees/pki/pkiactionplan.pdf, consultado el 12 de abril de 2007.

[14] Por ejemplo, el ETSI ha establecido una norma (TS 102 231) para instaurar una estructura no jerárquica que, entre otras cosas, permite abordar el reconocimiento cruzado de dominios de ICP y, en consecuencia, de la validez de los certificados. En lo fundamental, la norma TS 102 231 especifica pautas para la presentación de información sobre la situación de un proveedor de servicios de certificación (llamado "proveedor de servicios de confianza mutua"). Reviste la forma de una lista firmada, la "lista de situación de los servicios de confianza mutua", como base para la presentación de esa información. La lista de situación de servicios de confianza mutua especificada por el ETSI satisface el requisito de ofrecer pruebas sobre si el proveedor de un servicio de confianza mutua actúa o actuaba bajo la aprobación de un sistema reconocido cualquiera bien en el momento de prestarse el servicio, o en el momento en que se realizó una operación confiando en ese servicio. Para cumplir este requisito la lista de situación del servicio de confianza mutua ha de contener información por la cual sea posible determinar si el gestor del sistema conoció la intervención del proveedor de servicios de certificación en el momento de la operación y, en tal caso, cuál era la situación del servicio (es decir, si estaba aprobado, suspendido, cancelado o revocado). Por consiguiente, la lista de situación del servicio de confianza mutua contemplada en la norma técnica TS 102 231 del ETSI ha de contener no sólo la situación actual del servicio, sino además la historia de su situación. En consecuencia, la lista se convierte en una combinación de servicios válidos ("lista blanca") y servicios cancelados o revocados ("lista negra") (véase http://portal.etsi.org/stfs/STF_HomePages/STF 290/draft_ts_102231v010201p&RGW.doc. consultado el 4 de marzo de 2007).

se centra en los requisitos jurídicos formales y sustantivos para el reconocimiento transfronterizo de las firmas electrónicas.

1. Lugar de origen, reciprocidad y validación a nivel nacional

17. El lugar de origen es un factor clásico a la hora de otorgar reconocimiento jurídico a los documentos o escritos del extranjero. Esto se hace habitualmente sobre la base de la reciprocidad, de forma que se concede efecto en el ámbito nacional propio a las firmas y certificados de un país determinado en la medida en que el otro país da efecto legal a las firmas y certificados nacionales. Otro factor conexo es supeditar el efecto interno de la firma o el certificado de origen extranjero a alguna forma de validación o reconocimiento por parte de un proveedor de servicios de certificación, una autoridad de certificación o una entidad reguladora nacional[15].

18. No es corriente que las leyes internas denieguen expresamente el reconocimiento legal de las firmas o certificados extranjeros, lo que puede confirmar su carácter en apariencia no discriminatorio. Sin embargo, en la práctica, son muchos los regímenes de reconocimiento que suelen tener algún efecto discriminatorio, incluso no premeditado. Por ejemplo, la Directiva de la Unión Europea sobre la firma electrónica proscribe en general la discriminación de los certificados extranjeros que reúnan las condiciones (es decir, las firmas digitales basadas en una ICP). Sin embargo, esto redunda sobre todo en favor de los certificados emitidos por los proveedores de servicios de certificación establecidos en el territorio de los Estados miembros de la Unión Europea. Un proveedor de dichos servicios establecido en un tercer país tiene tres opciones para conseguir el reconocimiento de su certificado en la misma: cumplir los requisitos establecidos en la Directiva de la Unión Europea sobre la firma electrónica y obtener acreditación en el marco de un sistema establecido en un Estado miembro; concertar una certificación cruzada con un proveedor de servicios de certificación establecido en un Estado miembro de la comunidad europea; u operar al amparo de un reconocimiento general otorgado a nivel de un acuerdo internacional[16]. Por la forma en que la Directiva Europea regula los aspectos internacionales se colige que uno de sus objetivos era asegurar a los proveedores de servicios de certificación de la

---

[15] En la Argentina, por ejemplo, se reconocen los certificados y las firmas electrónicas de origen extranjero siempre que exista un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero o sean "reconocidos por un certificador licenciado en el país, y este reconocimiento sea validado por la autoridad de aplicación" (véase la Ley 25.506 de firma digital (2001) art. 16).

[16] En efecto, según lo dispuesto en el artículo 7 de la Directiva, los Estados miembros de la Unión Europea sólo deben velar por que los certificados expedidos por un proveedor de servicios de certificación establecido en un tercer país sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad siempre que a) el proveedor de servicios de certificación "cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro"; o b) un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva "avale" el certificado; o bien c) el certificado o el proveedor de servicios de certificación "estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales".

Unión Europea condiciones de acceso a los mercados extranjeros[17]. Al acumular el requisito de equivalencia sustancial a las normas de la Unión Europea más el requisito adicional de "acreditación en el marco de un sistema establecido en un Estado miembro", la Directiva de la Unión Europea sobre la firma electrónica exige de hecho que los proveedores de servicios de certificación extranjeros cumplan el régimen propio de partida más el de la Unión Europea, lo cual es un nivel más elevado que el exigido a los proveedores de servicios de certificación acreditados en un Estado miembro de la Unión[18].

19. El artículo 7 de la Directiva de la Unión Europea se ha aplicado con algunas variantes[19]. Irlanda y Malta, por ejemplo, reconocen las firmas digitales extranjeras (certificados reconocidos, según la terminología de la Unión) como equivalentes a las firmas nacionales siempre que satisfagan los demás requisitos jurídicos. En otros casos el reconocimiento está sujeto a verificación nacional (Austria, Luxemburgo) o a una decisión de una autoridad nacional (Estonia, Polonia, República Checa). Esta tendencia a insistir en alguna forma de verificación nacional, justificada en general por una legítima preocupación acerca del grado de fiabilidad de los certificados extranjeros, conduce en la práctica a un sistema de discriminación de los certificados extranjeros por razón de su origen geográfico.

2. Equivalencia sustancial

20. En consonancia con una vieja tradición, la CNUDMI declinó respaldar consideraciones de tipo geográfico a la hora de proponer factores para el reconocimiento de los certificados y las firmas electrónicas extranjeros. En efecto, el párrafo 1 del artículo 12 de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas estipula taxativamente que, al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, "no se tomará en consideración" ni "el lugar geográfico en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica" ni "el lugar geográfico en que se encuentre el establecimiento del expedidor o firmante".

21. El propósito del párrafo 1 del artículo 12 de la Ley Modelo de la UNCITRAL sobre las Firmas Electrónicas es dar reflejo al principio fundamental de que el lugar de origen no debe ser en modo alguno, de por sí, un factor determinante al decidir si los certificados o las firmas electrónicas de origen extranjero deben reconocerse susceptibles de producir efectos jurídicos, o en qué medida los producen. La determinación de si un certificado o una firma electrónica es susceptible de eficacia jurídica, o en qué medida lo es, debe depender de su fiabilidad técnica y no del lugar de su expedición. En algunos regímenes nacionales, por ejemplo en la Ley 2000 de

---

[17] El interés por asegurar el acceso de los proveedores de servicios de certificación europeos a los mercados extranjeros se desprende claramente de la formulación del párrafo 3 del artículo 7 de la Directiva, el cual estipula que "[c]uando la Comisión sea informada de cualquier dificultad encontrada por las empresas comunitarias en relación con el acceso al mercado en terceros países, podrá en caso necesario presentar propuestas al Consejo para obtener un mandato adecuado para la negociación de derechos comparables para las empresas comunitarias en dichos terceros países".

[18] Jos Dumortier y otros, "The legal and market aspects of electronic signatures", Estudio para la Dirección General de Sociedad de la Información de la Comisión Europea (Katholieke Universiteit Leuven, 2003), pág.58.

[19] Ibíd., págs. 92 a 94.

los Estados Unidos sobre las firmas electrónicas en el comercio mundial y nacional[20], existen también disposiciones no discriminatorias similares a las del artículo 12 de la Ley Modelo sobre las Firmas Electrónicas. Tales disposiciones estipulan que el lugar de origen, de por sí, no debe ser un factor al determinar si los certificados o las firmas electrónicas extranjeros deben reconocerse como susceptibles de eficacia jurídica en un Estado promulgante, o en qué medida los producen. Dichas disposiciones reconocen que la efectividad jurídica de un certificado o una firma electrónica debe depender de su fiabilidad técnica[21].

22. En lugar de los factores geográficos, la Ley Modelo establece una prueba de equivalencia sustancial entre los grados de fiabilidad ofrecidos por los certificados y firmas en cuestión. En consecuencia, si el certificado extranjero expedido presenta "un grado de fiabilidad sustancialmente equivalente" al de un certificado expedido en el Estado promulgante, tendrá "los mismos efectos jurídicos". De igual modo, una firma electrónica creada o utilizada fuera del país "producirá los mismos efectos jurídicos" que una firma electrónica creada o utilizada en el país "si presenta un grado de fiabilidad sustancialmente equivalente". La equivalencia entre los grados de fiabilidad presentados por los certificados y firmas nacionales y extranjeros ha de ser determinada en conformidad con normas internacionales reconocidas y cualquier otro factor pertinente, en particular un acuerdo entre las partes para utilizar ciertos tipos de firmas o certificados electrónicos, a no ser que el acuerdo carezca de validez o efectividad con arreglo al derecho aplicable.

23. La Ley Modelo no prescribe ni propugna convenios de reciprocidad. En efecto, la ley Modelo "no prevé nada en concreto" en cuanto a las técnicas jurídicas mediante las cuales un Estado promulgante pudiera reconocer por adelantado la fiabilidad de los certificados y las firmas que cumpliesen la legislación de un país extranjero (por ejemplo, una declaración unilateral o un tratado)"[22]. Los posibles métodos para alcanzar este resultado que se mencionaron al elaborar la Ley Modelo fueron, por ejemplo, el reconocimiento automático de las firmas que cumplieran las leyes de otro Estado si las leyes del Estado extranjero exigían un nivel de fiabilidad al menos equivalente al requerido para las firmas nacionales equivalentes. Otras técnicas legales mediante las cuales un Estado promulgante pudiera reconocer por anticipado la fiabilidad de los certificados y firmas extranjeros podrían ser declaraciones unilaterales o tratados[23].

---

[20] Véase la nota [...] [Código de los Estados Unidos, título 15, capítulo 96, sección 7031 (Principios que rigen la utilización de las firmas electrónicas en las operaciones internacionales)].

[21] Véase *Ley Modelo de la CNUDMI sobre las Firmas Electrónicas y Guía para su Incorporación*, segunda parte, párr. 83.

[22] Ibíd., párr. 157.

[23] Véase el informe del Grupo de Trabajo sobre comercio electrónico acerca de la labor de su 37º período de sesiones (A/CN.9/483), párrs. 39 y 42.